

14a

HEADER		DATA					
0	4	8	16	20	24	31 Bit	
VERS	HLEN	SERVICE TYPE		TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET			
TIME TO LIVE		PROTOCOL		HEADER CHECKSUM			
			SOURCE IP ADDRESS-0x0A80001				
			DESTINATION IP ADDRESS-0xA1C100001				
			IP OPTIONS (IF ANY)		PADDING		

32 Bits

14b

DATA ATTRIBUTE DESCRIPTION FIELD		ENCRYPTION DEFINITION FIELD
01 04 18 COA80000	05 18 AC100000 FF...	01 03 02 03 03 01 04 01
02 09 0034 55534552 09	0034 50415353 FF..	03 01 FF...
07 00 09 50 FF..		04 01 FF...
01 07 00 09 51 07 00 14	50 FF...	05 01 FF...
00 FF..		01 05 02 04 04 01 FF...

14c

INDEX	DATA ENCRYPTION ALGORITHM INDICATOR FIELD	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD
1	DES ENCRYPTION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR	0
2	DES ENCRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR
3	3DES ENCRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR
4	0	0	SHA1 AUTHENTICATION ALGORITHM INDICATOR
5	0	0	0

14d

HEADER	DECRYPTION INFORMATION DATA	CIPHERTEXT DATA
	DECRYPTION INFORMATION LABEL	DECRYPTION MODULE DATABASE INDEX=2

FIG.14